

CLAIMS

1. A method of performing numerical computations in a mathematical system comprising at least one function, the method comprising the steps of:
 - 5 - expressing the mathematical system in discrete terms,
 - expressing at least one variable of the mathematical system as a fixed-point number,
 - performing said computations in such a way that the computations include the at least one variable expressed as a fixed-point number,
 - obtaining, from said computations, a resulting number, the resulting number
- 10 representing at least one of:
 - a. at least a part of a solution to the mathematical system, and
 - b. a number usable in further computations involved in the numerical solution of the mathematical system,
 the method further comprising:
- 15 - extracting a set of data which represents at least one of:
 - i. a subset of digits of the resulting number, and
 - ii. a subset of digits of a number derived from the resulting number.
2. A method according to claim 1, wherein said set of data represent a pseudo-random
 20 number.
3. A method according to claim 1, wherein said computations involve at least a first and a second fixed-point number, each fixed-point number having a decimal separator, wherein the decimal separator of the first fixed-point number is positioned at a position different
 25 from the position of the decimal separator of the second fixed-point number.
4. A method according to claim 3, wherein the step of performing computations involves positioning the decimal separator of the first and second fixed-point number at selected positions.
- 30 5. A method according to claim 1, wherein said at least one function is non-linear.
6. A method according to claim 1, wherein the resulting number is expressed as a variable selected from the group consisting of:
 35 - an integer number,
- a floating point number, and
- a fixed-point number.
7. A method according to claim 1, wherein the mathematical system comprises at least
 40 one of:
 - a differential equation,
 - a discrete mapping.

8. A method according to claim 7, wherein the differential equation comprises at least one of:
- a partial differential equation,
 - an ordinary differential equation.
- 5
9. A method according to claim 7, wherein the discrete mapping comprises at least one of:
- an area-preserving map,
 - a non area-preserving map.
- 10
10. A method according to claim 7, wherein the mathematical system comprises at least one non-linear function governing at least one state variable X.
11. A method according to claim 10, wherein the mathematical system comprises a set of non-linear mapping functions.
- 15
12. A method according to claim 9, wherein the map comprises at least one of:
- a logistic map of the form:

$$x_{n+1} = \mu x_n (1 - x_n),$$
 - an Anosov map of the form:
- 20
- $$\begin{bmatrix} x_{n+1} \\ y_{n+1} \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ 1 & 2 \end{bmatrix} \begin{bmatrix} x_n \\ y_n \end{bmatrix} \bmod 1,$$
- a Hénon map of the form:

$$\begin{bmatrix} x_{n+1} \\ y_{n+1} \end{bmatrix} = \begin{bmatrix} 1 + y_n - ax_n^2 \\ bx_n \end{bmatrix}.$$
13. A method according to claim 1, wherein the mathematical system comprises at least
- 25 one non-linear differential equation.
14. A method according to claim 13, wherein the mathematical system comprises a set of non-linear differential equations.
- 30
15. A method according to claim 7, wherein the mathematical system has at least one positive Lyapunov exponent.
16. A method according to claim 7, comprising computing at least one Lyapunov exponent at least once during the mathematical computations.
- 35
17. A method according to claim 13, wherein the at least non-linear differential equation governs at least one state variable, X, which is a function of at least one independent variable, t.
- 40
18. A method according to claim 14, wherein the set of non-linear differential equations is a Lorenz system.

19. A method according to claim 18, wherein the Lorenz system consists of the following differential equations:

$$\begin{aligned}\frac{dx}{dt} &= \sigma(y - x) \\ \frac{dy}{dt} &= rx - y - xz, \\ \frac{dz}{dt} &= xy - bz,\end{aligned}$$

wherein $X=(x, y, z)$ are state variables, t is the independent variable, and σ , r and b are parameters.

20. A method according to claim 13, wherein the step of performing computations comprises numerically integrating at least one of:

- the non-linear differential equation, and
- 10 - the non-linear differential equations of said set of non-linear differential equations, by repeatedly computing a solution X_{n+1} based on at least one previous solution X_m , $m \leq n+1$, and a step length, Δt_n , of the independent variable, t .

21. A method according to claim 20, wherein the step of integrating comprises providing at least one initial condition, X_0 , of the state variable, X , and an initial step length, Δt_0 .

22. A method according to claim 10, wherein the step of performing computations comprises numerically iterating the non-linear mapping function.

23. A method according to claim 22, wherein the step of iterating comprises providing at least one initial condition, X_0 , of the state variable, X .

24. A method according to claim 20, wherein, in the discretized formulation of the Lorenz system, the solution X_{n+1} is computed using the step length $\Delta T = (\Delta t_{x,n}, \Delta t_{y,n}, \Delta t_{z,n})$ as follows:

$$\begin{aligned}x_{n+1} &= x_n + (\sigma(y_n - x_n)) \cdot \Delta t_{x,n} \\ y_{n+1} &= y_n + (x_n(r - z_n) - y_n) \cdot \Delta t_{y,n} \\ z_{n+1} &= z_n + (x_n y_n - b z_n) \cdot \Delta t_{z,n}\end{aligned}$$

wherein:

$\Delta t_{x,n}$ is the step length used in the computation of x_{n+1} ,

$\Delta t_{y,n}$ is the step length used in the computation of y_{n+1} ,

30 $\Delta t_{z,n}$ is the step length used in the computation of z_{n+1} .

25. A method according to claim 20, wherein the step length ΔT is constant throughout the computations.

26. A method according to claim 20, wherein, in each integration step, at least one of the elements $(\Delta t_{x,n}, \Delta t_{y,n}, \Delta t_{z,n})$ of the step length ΔT is a function of at least one number related to said computations.

27. A method according to claim 26, wherein, in each integration step, at least one of the elements ($\Delta t_{x,n}$, $\Delta t_{y,n}$, $\Delta t_{z,n}$) of the step length ΔT is a function of at least one solution, X_m , which is a solution to the mathematical system.

- 5 28. A method according to claim 26 wherein, in each integration step, at least one of the elements ($\Delta t_{x,n}$, $\Delta t_{y,n}$, $\Delta t_{z,n}$) of the step length ΔT is a function of at least one given step length, ΔT_m .

29. A method according to claim 1, wherein a key selected from an encryption key and a
10 decryption key is used to determine at least one value of at least one variable in the mathematical system.

30. A method according to claim 29, wherein the key is used to determine at least a part
of the initial condition X_0 .

15

31. A method according to claim 29, wherein the key is used to determine at least a part
of the initial step length ΔT_0 .

32. A method according to claim 29, wherein the key is used to determine the at least a
20 part of at least one of the parameters.

33. A method according to claim 29, wherein the key is a public key.

34. A method according to claim 29, wherein the key is a private key.

25

35. A method according to claim 1, comprising extracting a plurality of numbers resulting
from the computations.

36. A method according to claim 1, wherein the step of extracting comprises extracting at
30 least one number derived from k bits of the resulting number.

37. A method according to claim 1, wherein the step of extracting comprises extracting the
k least significant bits of the resulting number.

38. A method according to claim 36, wherein k is a value selected from the group
consisting of: 8, 16, 32, 64, and 128.

39. A method according to claim 36, wherein a plurality of numbers are extracted.

- 40 40. A method according to claim 1, wherein the extracted set of data is manipulated by
means of at least one of:
- an arithmetic operation, and
- a logical operation,
so as to obtain a combined set of data.

41. A method according to claim 40, wherein at least one of the:
- extracted set of data, and
 - the combined set of data
- 5 is combined with original data, so as to encrypt the original data.
42. A method according to claim 40, wherein at least one of:
- extracted set of data, and
 - the combined set of data
- 10 is combined with encrypted data, so as to decrypt the encrypted data and obtain the original data.
43. A method according to claim 40, wherein the combining of data comprises an XOR operation.
- 15
44. A method according to claim 1, wherein said computations involve data representing a block of plaintext in a block-cipher encryption and decryption system.
45. A method according to claim 1, wherein the extracted set of data is used to define at
- 20 least one operation on a block of plaintext in a block-cipher encryption and decryption system.
46. A method according to claim 41, wherein the combining of data comprises addition of the original data and the combined set of data for encryption, and subtraction of the
- 25 combined set of data from the encrypted data for decryption.
47. A method according to claim 41, wherein the combining of data comprises subtraction of the combined set of data from the original data for encryption, and addition of the combined set of data and the encrypted data for decryption.
- 30
48. A method according to claim 1, wherein the extracted set of data is used as at least one of: an encryption key and a decryption key.
49. A method according to claim 1, wherein the extracted set of data is used to generate
- 35 at least one of: an encryption key and a decryption key.
50. A method according to claim 1, wherein the extracted set of data is used in generation of data representing a digital signature.
- 40
51. A method according to claim 1, wherein the extracted set of data is used in watermarking of digital data.

52. A method according to claim 1, wherein the computations are performed on an electronic device which comprises an electronic processing unit having a register width, the method comprising the steps of:

- expressing at least one integer number of a bit width larger than said register width as at least two sub-numbers each having a bit width which is at most equal to said register width,
- performing at least one of said computations as a sub-computation on each of the sub-numbers so as to arrive at at least two partial results, expressed as integer numbers of a bit width smaller which is at most equal to the register width of the processing unit,
- concatenating the partial results to yield a representation of a result of said at least one computation.

53. A computer program for performing numerical computations in a mathematical system comprising at least one function, the computer program being adapted to:

- express at least one variable of the mathematical system as a fixed-point number,
- perform said computations in such a way that the computations include the at least one variable expressed as a fixed-point number,
- obtain, from said computations, a resulting number, the resulting number representing at least one of:
 - a. at least a part of a solution to the mathematical system, and
 - b. a number usable in further computations involved in the numerical solution of the mathematical system,

the computer program being further adapted to:

- extract a set of data which represents at least one of:
 - i. a subset of digits of the resulting number, and
 - ii. a subset of digits of a number derived from the resulting number.

54. A computer readable data carrier loaded with a computer program for performing numerical computations in a mathematical system comprising at least one function, the

computer program being adapted to:

- express at least one variable of the mathematical system as a fixed-point number,
- perform said computations in such a way that the computations include the at least one variable expressed as a fixed-point number,
- obtain, from said computations, a resulting number, the resulting number representing at least one of:
 - a. at least a part of a solution to the mathematical system, and
 - b. a number usable in further computations involved in the numerical solution of the mathematical system,

the computer program being further adapted to:

- extract a set of data which represents at least one of:
 - i. a subset of digits of the resulting number, and
 - ii. a subset of digits of a number derived from the resulting number.

55. A computer which is operatively connected to a computer readable data carrier loaded with a computer program for performing numerical computations in a mathematical system comprising at least one function, the computer program being adapted to:

- express at least one variable of the mathematical system as a fixed-point number,
 - 5 - perform said computations in such a way that the computations include the at least one variable expressed as a fixed-point number,
 - obtain, from said computations, a resulting number, the resulting number representing at least one of:
 - a. at least a part of a solution to the mathematical system, and
 - 10 - b. a number usable in further computations involved in the numerical solution of the mathematical system,
- the computer program being further adapted to:
- extract a set of data which represents at least one of:
 - i. a subset of digits of the resulting number, and
 - 15 - ii. a subset of digits of a number derived from the resulting number,
- wherein the computer comprises processor means for running said program.

56. A signal comprising an extracted set of data which have been derived from computations in a mathematical system, wherein, in order to arrive at the extracted set of data:

- 20 - the mathematical system has been expressed in discrete terms,
 - at least one variable of the mathematical system has been expressed as a fixed-point number,
 - said computations have been performed in such a way that the computations have
 - 25 included the at least one variable expressed as a fixed-point number,
 - a resulting number has been obtained from said computations, the resulting number representing at least one of:
 - a. at least a part of a solution to the mathematical system, and
 - b. a number usable in further computations involved in the numerical solution of
 - 30 the mathematical system,
- whereby the extracted set of data represents at least one of:
- i. a subset of digits of the resulting number, and
 - ii. a subset of digits of a number derived from the resulting number.

35 57. A signal comprising an encrypted set of data which has been derived as a combination of plaintext and at least one set of data extracted from computations in a mathematical system, wherein, in order to arrive at the extracted set of data:

- the mathematical system has been expressed in discrete terms,
- 40 - at least one variable of the mathematical system has been expressed as a fixed-point number,
- said computations have been performed in such a way that the computations have included the at least one variable expressed as a fixed-point number,
- a resulting number has been obtained from said computations, the resulting number representing at least one of:

- a. at least a part of a solution to the mathematical system, and
- b. a number usable in further computations involved in the numerical solution of the mathematical system,

whereby the extracted set of data represents at least one of:

- 5 - i. a subset of digits of the resulting number, and
- ii. a subset of digits of a number derived from the resulting number.

58. A method of detecting periodic behavior in the solution of a mathematical system comprising at least one non-linear function governing at least one state variable with
- 10 respect to at least one independent variable, the method comprising:
- expressing the mathematical system in discrete terms,
 - performing computations in an electronic device so as to obtain resulting numbers, the resulting numbers representing at least parts of solutions to the mathematical system,
 - storing selected solutions in an array, A, in a memory of the electronic device, the

15 array being adapted to store a finite number, $n+1$, of solutions,

 - determining whether at least one of:
 - a current solution, and
 - a particular one of said solutions stored in the array
 is substantially identical to another solution stored in the array.

- 20 59. A method according to claim 58, wherein only selected solutions are stored in the memory.

60. A method according to claim 58, wherein each entry in said array contains a solution
- 25 having an age which is growing by array level, A, 0 to n , the method comprising:
- at the step of storing selected solutions in the array: storing a current solution at the 0'th level in the array, A, thereby overwriting an old value stored at the 0'th level in the array, A,
 - if a 0'th predetermined criterion is fulfilled: transferring the old value to the 1'st level

30 in the array, A, before the 0'th level is overwritten by the current solution, and

for the 1'st level and each further level i in the array:

 - If an i 'th predetermined criterion for level i is fulfilled: transferring the old value stored at the i 'th level to the $i+1$ 'st level in the array, A, before the i 'th level is overwritten by the value transferred from the $i-1$ 'st level,

35 if the n 'th level is to be updated: discarding the old value previously stored at the n 'th level.

61. A method according to claim 60, further comprising, for each level, i , in the array, counting the number of times an old value stored at the i 'th level has been overwritten by
- 40 a new value without the old value being transferred to the $i+1$ 'st level, the i 'th predetermined criterion being fulfilled if the old value has not been transferred for a predetermined number of times.

62. A method according to claim 61, wherein the predetermined number of times is the same for all levels of the array, A.

63. A method according to claim 61, wherein the predetermined number of times varies
5 between the levels of the array, A.

64. A method according to claim 61, wherein the predetermined number of times for the i'th level of the array, A, is dependent from at least one value stored in the array.

10 65. A method according to claim 58, wherein said step of determining is only performed when a test criterion is fulfilled.

66. A method according to claim 65, wherein the test criterion is fulfilled when the sign of
15 at least one state variable changes.

67. A method according to claim 66, further comprising computing at least one derivative of at least one state variable with respect to one of said at least one independent variable, the test criterion being fulfilled when there occurs a change of sign of said at least one
20 derivative.

68. A method according to claim 66, further comprising computing a test value from at least one of:

- said at least one state variable, and
- said derivative,

25 the test criterion being based on the test value.

69. A method of generating a pseudo-random number, the method comprising:

I) expressing a mathematical system in discrete terms,

II) defining a seed value representing at least an initial condition for the mathematical
30 system,

III) expressing at least one variable of the mathematical system as a fixed-point number,

IV) performing computations in an electronic device, the computations including the at least one variable expressed as a fixed-point number and obtaining, from said computations, a resulting number, the resulting number representing at least one of:

35 a. at least a part of a solution to the mathematical system, and
b. a number usable in further computations involved in the numerical solution of the mathematical system,

V) extracting, as the pseudo-random number, a number derived from at least one number which has occurred during the computations.

40 70. A method according to claim 69, wherein the pseudo-random number is extracted as a number derived from k digits of said at least one number which has occurred during the computations.

71. A method according to claim 70, wherein the pseudo-random number is extracted as a number derived from the k least significant digits of said at least one number.

72. A method according to claim 69, the method comprising the steps of repeating steps IV) and V) until a given amount of pseudo-random numbers has been generated.

73. A method according to claim 69, wherein a given amount of pseudo-random numbers is generated and stored in a memory of the electronic device as a spare seed value.

74. A method according to claim 69, wherein a plurality of resulting numbers are obtained which represent at least parts of solutions to the mathematical system, the method further comprising detecting periodic behavior in the solution of the mathematical system, the mathematical system comprising at least one non-linear function governing at least one state variable with respect to at least one independent variable, the detecting of periodic behavior comprising:

- storing selected solutions in an array, A, in a memory of the electronic device, the array being adapted to store a finite number, n+1, of solutions,
- determining whether at least one of:

- a current solution, and

- a particular one of said solutions stored in the array

is substantially identical to another solution stored in the array,

the method further comprising:

if the step of determining reveals that at least one of

- the current solution, and
- the particular solution

is identical to another solution:

interrupting the pseudo-random-number generation, i.e. interrupting repetition of steps IV) and V),

using the spare seed value as the seed value in the step II),

resuming the pseudo-random-number generation, i.e. resuming repetition of steps IV) and V).

75. A method according to claim 74, further comprising, prior to the step of resuming the pseudo-random number generation, generating and storing, in a memory of the electronic device, a given amount of pseudo-random numbers as a new spare seed value.

76. A method according to claim 69, wherein each level in the array, A, is reset prior to step IV), when steps IV) and V) are initiated with a new seed value at step II).

77. A method of encrypting a set of original data into a set of encrypted data, the method comprising the steps of:

A) generating a pseudo-random number by performing the steps of:

I) expressing a mathematical system in discrete terms,

- II) defining an encryption key representing at least an initial condition for the mathematical system,
 III) expressing at least one variable of the mathematical system as a fixed-point number,
 5 IV) performing computations including the at least one variable expressed as a fixed-point number and obtaining, from the computations, a resulting number, the resulting number representing at least one of:
 a. at least a part of a solution to the mathematical system, and
 b. a number usable in further computations involved in the numerical solution of the mathematical system,
 10 V) extracting, as the pseudo-random number, a number derived from at least one number which has occurred during the computations,
 B) manipulating the original data and the pseudo-random number by means of at least one of:
 15 i. an arithmetic operation, and
 ii. a logical operation,
 so as to obtain a combined set of data, the combined set of data being the encrypted data.
78. A method according to claim 77, wherein, prior to step A), a sub-set of the original
 20 data is separated from the set of data, and wherein step B) is performed on the sub-set of data.
79. A method according to claim 77, wherein the pseudo-random number is extracted as a number derived from k digits of said at least one number which has occurred during the
 25 computations.
80. A method according to claim 77, wherein the pseudo-random number is extracted as a number derived from the k least significant digits of said at least one number which has occurred during the computations.
 30
81. A method according to claim 77, the method comprising the steps of repeating steps IV) and V) until a given amount of pseudo-random numbers has been generated.
82. A method according to claim 77, wherein a given amount of pseudo-random numbers
 35 is generated and stored in a memory of the electronic device as a spare encryption key.
83. A method according to claim 82, wherein a plurality of resulting numbers are obtained which represent at least parts of solutions to the mathematical system, the method further comprising detecting periodic behavior in the solution of the mathematical system, the
 40 mathematical system comprising at least one non-linear function governing at least one state variable with respect to at least one independent variable, the detecting of periodic behavior comprising:
 - storing selected solutions in an array, A, in a memory of the electronic device, the array being adapted to store a finite number, $r+1$, of solutions,

- determining whether at least one of:
 - a current solution, and
 - a particular one of said solutions stored in the array
 is substantially identical to another solution stored in the array,
- 5 the method further comprising:
 - if the step of determining reveals that at least one of:
 - the current solution, and
 - the particular solution
 is identical to another solution:
- 10 - interrupting the pseudo-random number generation, i.e. interrupting repetition of steps IV) and V),
 - using the spare encryption key as the encryption key in step II),
 - resuming the pseudo-random number generation, i.e. resuming repetition of steps IV) and V).
- 15 84. A method according to claim 83, further comprising, prior to the step of resuming the pseudo-random number generation, generating and storing, in a memory of the electronic device, a given amount of pseudo-random numbers as a new spare encryption key.
- 20 85. A method according to claim 77, wherein each level in the array, A, is reset prior to step IV), when steps IV) and V) are initiated with a new seed value at step II).
- 86. A method of decrypting a set of encrypted data which has been encrypted by a method of encrypting a set of original data into said set of encrypted data, the method of
 - 25 encrypting comprising the steps of:
 - A) generating a pseudo-random number by performing the steps of:
 - I) expressing a mathematical system in discrete terms,
 - II) defining an encryption key representing at least an initial condition for the mathematical system,
 - 30 III) expressing at least one variable of the mathematical system as a fixed-point number,
 - IV) performing computations including the at least one variable expressed as a fixed-point number and obtaining, from the computations, a resulting number, the resulting number representing at least one of:
 - 35 a. at least a part of a solution to the mathematical system, and
 - b. a number usable in further computations involved in the numerical solution of the mathematical system,
 - V) extracting, as the pseudo-random number, a number derived from at least one number which has occurred during the computations,
 - 40 B) manipulating the original data and the pseudo-random number by means of at least one of:
 - i. an arithmetic operation, and
 - ii. a logical operation,
 so as to obtain a combined set of data, the combined set of data being the encrypted data,

the method of decrypting comprising the steps of:

a) performing step A), so as to extract the same pseudo-random number as extracted in step V),

b) manipulating the encrypted data and the pseudo-random number by means of at least

5 one of:

- an arithmetic operation, and
- a logical operation,

so as to obtain the original, i.e. decrypted, version of the data.

10 87. A method according to claim 86, wherein, prior to step a), a sub-set of the encrypted data is separated from the set of encrypted data, the method of decrypting comprising performing steps a) and b) on said sub-set of data.

88. A method according to claim 87 comprising repeating the steps of claim 87 until a
15 plurality of sub-sets which in common constitute the entire set of encrypted data have been decrypted.

89. A computer program for encrypting and decrypting a set of data, the computer program being adapted to run in an encryption mode and in a decryption mode, the
20 computer program being further adapted to:

i) generate a pseudo-random number in a reproducible way by performing the steps of:

- expressing a mathematical system in discrete terms,
- expressing at least one variable of the mathematical system as a fixed-point number,
- performing computations including the at least one variable expressed as a fixed-point
25 number,

- obtaining, from the computations, a resulting number, the resulting number representing at least one of:

- a. a part of a solution to the mathematical system, and
- b. a number usable in further computations involved in the numerical solution of the
30 mathematical system,

- extracting, as the pseudo-random number, a number derived from at least one number which has occurred during the computations,

ii) manipulate the data and the pseudo-random number by means of at least one of:

- an arithmetic operation, and
- a logical operation,

35 so as to obtain a combined set of data, wherein:

- the combined set of data represents an encrypted version of the data in case the computer program is run in encryption mode,
- the combined set of data represents a decrypted version of the data in case the
40 computer program is run in decryption mode.

90. A computer readable data carrier loaded with a computer program for encrypting and decrypting a set of data, the computer program being adapted to run in an encryption mode and in a decryption mode, the computer program being further adapted to:

- i) generate a pseudo-random number in a reproducible way by performing the steps of:
 - expressing a mathematical system in discrete terms,
 - expressing at least one variable of the mathematical system as a fixed-point number,
 - performing computations including the at least one variable expressed as a fixed-point number,
- 5 - obtaining, from the computations, a resulting number, the resulting number representing at least one of:
 - a. a part of a solution to the mathematical system, and
 - b. a number usable in further computations involved in the numerical solution of the mathematical system,
- 10 - extracting, as the pseudo-random number, a number derived from at least one number which has occurred during the computations,
- ii) manipulate the data and the pseudo-random number by means of at least one of:
 - an arithmetic operation, and
 - 15 - a logical operation,
- so as to obtain a combined set of data, wherein:
 - the combined set of data represents an encrypted version of the data in case the computer program is run in encryption mode,
 - the combined set of data represents a decrypted version of the data in case the computer
 - 20 program is run in decryption mode.

91. A computer being operatively connected to a computer readable data carrier loaded with a computer program for encrypting and decrypting a set of data, the computer program being adapted to run in an encryption mode and in a decryption mode, the
- 25 computer program being further adapted to:
- i) generate a pseudo-random number in a reproducible way by performing the steps of:
 - expressing a mathematical system in discrete terms,
 - expressing at least one variable of the mathematical system as a fixed-point number,
 - performing computations including the at least one variable expressed as a fixed-point number,
 - 30 - obtaining, from the computations, a resulting number, the resulting number representing at least one of:
 - a. a part of a solution to the mathematical system, and
 - b. a number usable in further computations involved in the numerical solution of the mathematical system,
 - 35 - extracting, as the pseudo-random number, a number derived from at least one number which has occurred during the computations,
 - ii) manipulate the data and the pseudo-random number by means of at least one of:
 - an arithmetic operation, and
 - 40 - a logical operation,
 - so as to obtain a combined set of data, wherein:
 - the combined set of data represents an encrypted version of the data in case the computer program is run in encryption mode,

the combined set of data represents a decrypted version of the data in case the computer program is run in decryption mode, the computer comprising processor means for running said program.

- 5 92. A method of generating a pseudo-random number, the method comprising, in one instance:
- 1) expressing a mathematical system in discrete terms,
 II) defining a seed value representing at least an initial condition for the mathematical system,
- 10 III) expressing at least one variable of the mathematical system as a fixed-point number,
 IV) performing computations including the at least one variable expressed as a fixed-point number and obtaining a resulting number, the resulting number representing at least one of:
- a. a part of a solution to the mathematical system, and
 15 b. a number usable in further computations involved in the numerical solution of the mathematical system,
 V) extracting, as the pseudo-random number, a number derived from at least one number which has occurred during the computations, performing steps I) - V) in a plurality of instances in parallel.
- 20 93. A method according to claim 92, comprising transmitting data between the plurality of instances at least while performing step IV) for each of the instances.
94. A method according to claim 92, further comprising transmitting data between the
 25 plurality of instances while performing step V) for each of the instances.
95. A method according to claim 92, comprising combining, by use of at least one of:
- an arithmetic operation, and
 - a logical operation,
- 30 a plurality of pseudo-random numbers extracted at step V) in each of the instances into a common pseudo-random number.
96. A method of performing numerical computations in a mathematical system comprising at least one function, the method comprising the steps of:
- 35 - expressing the mathematical system in discrete terms,
 - expressing at least one variable of the mathematical system as a fixed-point number,
 - performing said computations in such a way that the computations include the at least one variable expressed as a fixed-point number,
 - obtaining, from said computations, a resulting number, the resulting number
 40 representing at least one of:
- a. at least a part of a solution to the mathematical system, and
 b. a number usable in further computations involved in the numerical solution of the mathematical system,
- the step of performing computations comprising:

- repeatedly computing a solution X_{n+1} based on at least one previous solutions X_m , $m \leq n-1$, whereby the step of performing computations is initiated based on at least one initial condition, X_0 , of the state variable, X ,

the method further comprising:

- 5 - providing a cryptographic key as an input to said computations, whereby the cryptographic key is used in generation of the initial condition X_0 .

97. A method of determining an identification value for identifying a set of data, the method comprising performing numerical computations in a mathematical system

- 10 comprising at least one function, the method comprising the steps of:

- expressing the mathematical system in discrete terms,
- expressing at least one variable of the mathematical system as a fixed-point number,
- performing said computations in such a way that the computations include the at least one variable expressed as a fixed-point number,

- 15 - obtaining, from said computations, a resulting number, the resulting number representing at least one of:

- a. at least a part of a solution to the mathematical system, and
- b. a number usable in further computations involved in the numerical solution of the mathematical system,

- 20 whereby a representation of at least part of the set of data is used in said computations, the method further comprising:

- extracting, as said identification value, at least a part of said resulting number.

98. A method according to claim 97, wherein a cryptographic key is used as a seed value

- 25 for the computations.

99. A method according to claim 97, wherein the mathematical system comprises at least one of:

- a differential equation,
- 30 - a discrete mapping.

100. A method according to claim 99, wherein the differential equation comprises at least one of:

- a partial differential equation,
- 35 - an ordinary differential equation.

101. A method according to claim 99, wherein the discrete mapping comprises at least one of:

- an area-preserving map,
- 40 - a non area-preserving map.

102. A method according to claim 99, wherein the mathematical system comprises at least one non-linear function governing at least one state variable X .

103. A method according to claim 102, wherein the non-linear mapping function comprises a logistic map of the form $x_{n+1} = \lambda x_n(1-x_n)$, wherein λ is a parameter, x_{n+1} is the value of state variable x at the $(n+1)$ 'th stage in the computations, and x_n is the value of state variable x at the n 'th stage in the computations.

5

104. A method according to claim 103, wherein the logistic map is modified into the form $x_{n+1} = \lambda x_n(1-x_n) + \epsilon(x_n - m_n)$, wherein λ and ϵ are parameters, x_{n+1} is the value of state variable x at the $(n+1)$ 'th stage in the computations, x_n is the value of state variable x at the n 'th stage in the computations, and m_n contains a representation of an n 'th portion of the set of data.

10

105. A method according to claim 103, wherein a cryptographic key is used for at least partially determining at least one of the following: λ , ϵ and an initial value x_0 of state variable x .

15

106. A method according to claim 97, wherein the mathematical system comprises a set of non-linear mapping functions.

107. A method according to claim 106, wherein the set of mapping functions comprises at least one of:

20

– an Anosov map of the form:

$$\begin{bmatrix} x_{n+1} \\ y_{n+1} \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ 1 & 2 \end{bmatrix} \begin{bmatrix} x_n \\ y_n \end{bmatrix} \bmod 1,$$

– a Hénon map of the form:

$$\begin{bmatrix} x_{n+1} \\ y_{n+1} \end{bmatrix} = \begin{bmatrix} 1 + y_n - ax_n^2 \\ bx_n \end{bmatrix}.$$

25

108. A method according to claim 97, wherein the mathematical system comprises at least one non-linear differential equation.

109. A method according to claim 108, wherein the mathematical system comprises a set of non-linear differential equations.

30

110. A method according to claim 97, wherein the mathematical system has at least one positive Lyapunov exponent.

35 111. A method according to claim 97, comprising computing at least one Lyapunov exponent at least once during the mathematical computations.

112. A method according to claim 108, wherein the at least one non-linear differential equation governs at least one state variable, X , which is a function of at least one

40 independent variable, t .

113. A method according to claim 109, wherein the set of non-linear differential equations comprises a Lorenz system.

114. A method of performing numerical computations in a mathematical system

- 5 comprising at least one function, the method comprising the steps of:
 - expressing the mathematical system in discrete terms,
 - restricting the range of at least a selected variable of said function, the range being sufficiently narrow so as to exclude values which the selected variable, by virtue of said function, would assume if not restricted by said range,
- 10 - performing computations so as to obtain a resulting number, the resulting number representing at least one of:
 - a. a part of a solution to the mathematical system, and
 - b. a number usable in further computations involved in the numerical solution of the mathematical system,
- 15 - when the computations result in a value for the selected variable which is beyond the range, assigning a value within the range to the selected variable.

115. A method according to claim 114, wherein the method is a part of a pseudo-random number generating method.

20

116. A method according to claim 115, wherein the pseudo-random number generating method generates pseudo-random numbers for use in at least one of encryption and decryption.

- 25 117. A method according to claim 114, wherein the mathematical system has at least one positive Lyapunov exponent.

118. A method of performing numerical computations in a mathematical system comprising at least one function, the method comprising the steps of:

- 30 - expressing the mathematical system in discrete terms,
- expressing at least one variable of the mathematical system as an integer number,
- placing an imaginary decimal separator in said integer number, whereby the integer number represents a real number,
- performing computations including the at least one variable expressed as an integer number so as to obtain a resulting number, the resulting number being expressed as an integer number,
- 35 - positioning the imaginary decimal separator in the resulting number at a predetermined position by performing at least one of the steps of:
 - correcting the position of the imaginary decimal separator in the integer number, and
 - placing an imaginary separator in the resulting number.
- 40

119. A method of performing numerical computations in a mathematical system comprising at least one function, the method comprising the steps of:

- expressing the mathematical system in discrete terms,
 - expressing at least one variable of the mathematical system as a fixed-point number,
 - performing said computations in such a way that the computations include the at least one variable expressed as a fixed-point number,
- 5 - obtaining, from said computations, a resulting number, the resulting number representing at least one of:
- a. at least a part of a solution to the mathematical system, and
 - b. a number usable in further computations involved in the numerical solution of the mathematical system.

10

10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28
29
30
31
32
33
34
35
36
37
38
39
40
41
42
43
44
45
46
47
48
49
50
51
52
53
54
55
56
57
58
59
60
61
62
63
64
65
66
67
68
69
70
71
72
73
74
75
76
77
78
79
80
81
82
83
84
85
86
87
88
89
90
91
92
93
94
95
96
97
98
99
100
101
102
103
104
105
106
107
108
109
110
111
112
113
114
115
116
117
118
119
120
121
122
123
124
125
126
127
128
129
130
131
132
133
134
135
136
137
138
139
140
141
142
143
144
145
146
147
148
149
150
151
152
153
154
155
156
157
158
159
160
161
162
163
164
165
166
167
168
169
170
171
172
173
174
175
176
177
178
179
180
181
182
183
184
185
186
187
188
189
190
191
192
193
194
195
196
197
198
199
200
201
202
203
204
205
206
207
208
209
210
211
212
213
214
215
216
217
218
219
220
221
222
223
224
225
226
227
228
229
230
231
232
233
234
235
236
237
238
239
240
241
242
243
244
245
246
247
248
249
250
251
252
253
254
255
256
257
258
259
260
261
262
263
264
265
266
267
268
269
270
271
272
273
274
275
276
277
278
279
280
281
282
283
284
285
286
287
288
289
290
291
292
293
294
295
296
297
298
299
300
301
302
303
304
305
306
307
308
309
310
311
312
313
314
315
316
317
318
319
320
321
322
323
324
325
326
327
328
329
330
331
332
333
334
335
336
337
338
339
340
341
342
343
344
345
346
347
348
349
350
351
352
353
354
355
356
357
358
359
360
361
362
363
364
365
366
367
368
369
370
371
372
373
374
375
376
377
378
379
380
381
382
383
384
385
386
387
388
389
390
391
392
393
394
395
396
397
398
399
400
401
402
403
404
405
406
407
408
409
410
411
412
413
414
415
416
417
418
419
420
421
422
423
424
425
426
427
428
429
430
431
432
433
434
435
436
437
438
439
440
441
442
443
444
445
446
447
448
449
450
451
452
453
454
455
456
457
458
459
460
461
462
463
464
465
466
467
468
469
470
471
472
473
474
475
476
477
478
479
480
481
482
483
484
485
486
487
488
489
490
491
492
493
494
495
496
497
498
499
500
501
502
503
504
505
506
507
508
509
510
511
512
513
514
515
516
517
518
519
520
521
522
523
524
525
526
527
528
529
530
531
532
533
534
535
536
537
538
539
540
541
542
543
544
545
546
547
548
549
550
551
552
553
554
555
556
557
558
559
560
561
562
563
564
565
566
567
568
569
570
571
572
573
574
575
576
577
578
579
580
581
582
583
584
585
586
587
588
589
590
591
592
593
594
595
596
597
598
599
600
601
602
603
604
605
606
607
608
609
610
611
612
613
614
615
616
617
618
619
620
621
622
623
624
625
626
627
628
629
630
631
632
633
634
635
636
637
638
639
640
641
642
643
644
645
646
647
648
649
650
651
652
653
654
655
656
657
658
659
660
661
662
663
664
665
666
667
668
669
670
671
672
673
674
675
676
677
678
679
680
681
682
683
684
685
686
687
688
689
690
691
692
693
694
695
696
697
698
699
700
701
702
703
704
705
706
707
708
709
710
711
712
713
714
715
716
717
718
719
720
721
722
723
724
725
726
727
728
729
730
731
732
733
734
735
736
737
738
739
740
741
742
743
744
745
746
747
748
749
750
751
752
753
754
755
756
757
758
759
760
761
762
763
764
765
766
767
768
769
770
771
772
773
774
775
776
777
778
779
780
781
782
783
784
785
786
787
788
789
790
791
792
793
794
795
796
797
798
799
800
801
802
803
804
805
806
807
808
809
810
811
812
813
814
815
816
817
818
819
820
821
822
823
824
825
826
827
828
829
830
831
832
833
834
835
836
837
838
839
840
841
842
843
844
845
846
847
848
849
850
851
852
853
854
855
856
857
858
859
860
861
862
863
864
865
866
867
868
869
870
871
872
873
874
875
876
877
878
879
880
881
882
883
884
885
886
887
888
889
890
891
892
893
894
895
896
897
898
899
900
901
902
903
904
905
906
907
908
909
910
911
912
913
914
915
916
917
918
919
920
921
922
923
924
925
926
927
928
929
930
931
932
933
934
935
936
937
938
939
940
941
942
943
944
945
946
947
948
949
950
951
952
953
954
955
956
957
958
959
960
961
962
963
964
965
966
967
968
969
970
971
972
973
974
975
976
977
978
979
980
981
982
983
984
985
986
987
988
989
990
991
992
993
994
995
996
997
998
999
1000
1001
1002
1003
1004
1005
1006
1007
1008
1009
1010
1011
1012
1013
1014
1015
1016
1017
1018
1019
1020
1021
1022
1023
1024
1025
1026
1027
1028
1029
1030
1031
1032
1033
1034
1035
1036
1037
1038
1039
1040
1041
1042
1043
1044
1045
1046
1047
1048
1049
1050
1051
1052
1053
1054
1055
1056
1057
1058
1059
1060
1061
1062
1063
1064
1065
1066
1067
1068
1069
1070
1071
1072
1073
1074
1075
1076
1077
1078
1079
1080
1081
1082
1083
1084
1085
1086
1087
1088
1089
1090
1091
1092
1093
1094
1095
1096
1097
1098
1099
1100
1101
1102
1103
1104
1105
1106
1107
1108
1109
1110
1111
1112
1113
1114
1115
1116
1117
1118
1119
1120
1121
1122
1123
1124
1125
1126
1127
1128
1129
1130
1131
1132
1133
1134
1135
1136
1137
1138
1139
1140
1141
1142
1143
1144
1145
1146
1147
1148
1149
1150
1151
1152
1153
1154
1155
1156
1157
1158
1159
1160
1161
1162
1163
1164
1165
1166
1167
1168
1169
1170
1171
1172
1173
1174
1175
1176
1177
1178
1179
1180
1181
1182
1183
1184
1185
1186
1187
1188
1189
1190
1191
1192
1193
1194
1195
1196
1197
1198
1199
1200
1201
1202
1203
1204
1205
1206
1207
1208
1209
1210
1211
1212
1213
1214
1215
1216
1217
1218
1219
1220
1221
1222
1223
1224
1225
1226
1227
1228
1229
1230
1231
1232
1233
1234
1235
1236
1237
1238
1239
1240
1241
1242
1243
1244
1245
1246
1247
1248
1249
1250
1251
1252
1253
1254
1255
1256
1257
1258
1259
1260
1261
1262
1263
1264
1265
1266
1267
1268
1269
1270
1271
1272
1273
1274
1275
1276
1277
1278
1279
1280
1281
1282
1283
1284
1285
1286
1287
1288
1289
1290
1291
1292
1293
1294
1295
1296
1297
1298
1299
1300
1301
1302
1303
1304
1305
1306
1307
1308
1309
1310
1311
1312
1313
1314
1315
1316
1317
1318
1319
1320
1321
1322
1323
1324
1325
1326
1327
1328
1329
1330
1331
1332
1333
1334
1335
1336
1337
1338
1339
1340
1341
1342
1343
1344
1345
1346
1347
1348
1349
1350
1351
1352
1353
1354
1355
1356
1357
1358
1359
1360
1361
1362
1363
1364
1365
1366
1367
1368
1369
1370
1371
1372
1373
1374
1375
1376
1377
1378
1379
1380
1381
1382
1383
1384
1385
1386
1387
1388
1389
1390
1391
1392
1393
1394
1395
1396
1397
1398
1399
1400
1401
1402
1403
1404
1405
1406
1407
1408
1409
1410
1411
1412
1413
1414
1415
1416
1417
1418
1419
1420
1421
1422
1423
1424
1425
1426
1427
1428
1429
1430
1431
1432
1433
1434
1435
1436
1437
1438
1439
1440
1441
1442
1443
1444
1445
1446
1447
1448
1449
1450
1451
1452
1453
1454
1455
1456
1457
1458
1459
1460
1461
1462
1463
1464
1465
1466
1467
1468
1469
1470
1471
1472
1473
1474
1475
1476
1477
1478
1479
1480
1481
1482
1483
1484
1485
1486
1487
1488
1489
1490
1491
1492
1493
1494
1495
1496
1497
1498
1499
1500
1501
1502
1503
1504
1505
1506
1507
1508
1509
1510
1511
1512
1513
1514
1515
1516
1517
1518
1519
1520
1521
1522
1523
1524
1525
1526
1527
1528
1529
1530
1531
1532
1533
1534
1535
1536
1537
1538
1539
1540
1541
1542
1543
1544
1545
1546
1547
1548
1549
1550
1551
1552
1553
1554
1555
1556
1557
1558
1559
1560
1561
1562
1563
1564
1565
1566
1567
1568
1569
1570
1571
1572
1573
1574
1575
1576
1577
1578
1579
1580
1581
1582
1583
1584
1585
1586
1587
1588
1589
1590
1591
1592
1593
1594
1595
1596
1597
1598
1599
1600
1601
1602
1603
1604
1605
1606
1607
1608
1609
1610
1611
1612
1613
1614
1615
1616
1617
1618
1619
1620
1621
1622
1623
1624
1625
1626
1627
1628
1629
1630
1631
1632
1633
1634
1635
1636
1637
1638
1639
1640
1641
1642
1643
1644
1645
1646
1647
1648
1649
1650
1651
1652
1653
1654
1655
1656
1657
1658
1659
1660
1661
1662
1663
1664
1665
1666
1667
1668
1669
1670
1671
1672
1673
1674
1675
1676
1677
1678
1679
1680
1681
1682
1683
1684
1685
1686
1687
1688
1689
1690
1691
1692
1693
1694
1695
1696
1697
1698
1699
1700
1701
1702
1703
1704
1705
1706
1707
1708
1709
1710
1711
1712
1713
1714
1715
1716
1717
1718
1719
1720
1721
1722
1723
1724
1725
1726
1727
1728
1729
1730
1731
1732
1733
1734
1735
1736
1737
1738
1739
1740
1741
1742
1743
1744
1745
1746
1747
1748
1749
1750
1751
1752
1753
1754
1755
1756
1757
1758
1759
1760
1761
1762
1763
1764
1765
1766
1767
1768
1769
1770
1771
1772
1773
1774
1775
1776
1777
1778
1779
1780
1781
1782
1783
1784
1785
1786
1787
1788
1789
1790
1791
1792
1793
1794
1795
1796
1797
1798
1799
1800
1801
1802
1803
1804
1805
1806
1807
1808
1809
1810
1811
1812
1813
1814
1815
1816
1817
1818
1819
1820
1821
1822
1823
1824
1825
1826
1827
1828
1829
1830
1831
1832
1833
1834
1835
1836
1837
1838
1839
1840
1841
1842
1843
1844
1845
1846
1847
1848
1849
1850
1851
1852
1853
1854
1855
1856
1857
1858
1859
1860
1861
1862
1863
1864
1865
1866
1867
1868
1869
1870
1871
1872
1873
1874
1875
1876
1877
1878
1879
1880
1881
1882
1883
1884
1885
1886
1887
1888
1889
1890
1891
1892
1893
1894
1895
1896
1897
1898
1899
1900
1901
1902
1903
1904
1905
1906
1907
1908
1909
1910
1911
1912
1913
1914
1915
1916
1917
1918
1919
1920
1921
1922
1923
1924
1925
1926
1927
1928
1929
1930
1931
1932
1933
1934
1935
1936
1937
1938
1939
1940
1941
1942
1943
1944
1945
1946
1947
1948
1949
1950
1951
1952
1953
1954
1955
1956
1957
1958
1959
1960
1961
1962
1963
1964
1965
1966
1967
1968
1969
1970
1971
1972
1973
1974
1975
1976
1977
1978
1979
1980
1981
1982
1983
1984
1985
1986
1987
1988
1989
1990
1991
1992
1993
1994
1995
1996
1997
1998
1999
2000
2001
2002
2003
2004
2005
2006
2007
2008
2009
2010
2011
2012
2013
2014
2015
2016
2017
2018
2019
2020
2021
2022
2023
2024
2025
2026
2027
2028
2029
2030
2031
2032
2033
2034
2035
2036
2037
2038
2039
2040
2041
2042
2043
2044
2045
2046
2047
2048
2049
2050
2051
2052
2053
2054
2055
2056
2057
2058
2059
2060
2061
2062
2063
2064
2065
2066
2067
2068
2069
2070
2071
2072
2073
2074
2075
2076
2077
2078
2079
2080
2081
2082
2083
2084
2085
2086
2087
2088
2089
2090
2091
2092
2093
2094
2095
2096
2097
2098
2099
2100
2101
2102
2103
2104
2105
2106
2107
2108
2109
2110
2111
2112
2113
2114
2115
2116
2117
2118
2119
2120
2121
2122
2123
2124
2125
2126
2127
2128
2129
2130
2131
2132
2133
2134
2135
2136
2137
2138
2139
2140
2141
2142
2143
2144
2145
2146
2147
2148
2149
2150
2151
2152
2153
2154
2155
2156
2157
2158
2159
2160
2161
2162
2163
2164
2165
2166
2167
2168
2169
2170
2171
2172
2173
2174
2175
2176
2177
2178
2179
2180
2181
2182
2183
2184
2185
2186
2187
2188
2189
2190
2191
2192
2193
2194
2195
2196
2197
2198
2199
2200
2201
2202
2203
2204
2205
2206
2207
2208
2209
22